AO 93 (Rev. 12/09) Search and Seizure Warrant (USAO CDCA Rev. 01/2013)

UNITED STATES DISTRICT COURT

for the

Central District of California

ORIGINAL

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
12959 Lasselle Street
Moreno Valley, California

Case No. ED15-0390M

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California
(identify the person or describe the property to be searched and give its location):

See Attachment A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 10/13/15, 7:15 p.m.

Judge's signature

City and state: Riverside, California

Hon. David T. Bristow, U.S. Magistrate Judge
Printed name and title

SAUSA: Teresa Beecham

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
15-0390	10/13/2015 2000 HRS	ANGELO HARPER, SR.

Inventory made in the presence of:
SA GEORGE ALEXIA

Inventory of the property taken and name of any person(s) seized:
[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]

1 – FOUR THUMBDRIVES
2 – ONE SD MEMORY CARD
3 – THREE SMARTPHONES
4 – TWO DESKTOP COMPUTERS
5 – ONE EXTERNAL HARD DRIVE

Certification (by officer present during the execution of the warrant)

I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.

Date: 11/2/15

Executing officer's signature

JOAQUIN RUIZ SPECIAL AGENT
Printed name and title

SAUSA: Teresa Beecham

UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
12959 Lasselle Street
Moreno Valley, California

Case No. ED15-0390M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S. Code, Sections 2251(a), 2252A(a)(2), 2252a(a)(5)(B),	See attached Affidavit

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jonathan Ruiz, HSI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/13/15

DAVID T. BRISTOW

Judge's signature

City and state: Riverside, California

Hon. David T. Bristow, U.S. Magistrate Judge

Printed name and title

Jennifer Juan for:
SAUSA Teresa Beecham

AFFIDAVIT

I, Jonathan Ruiz, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") and have been so employed since 2007. From April of 2007 to November of 2014, I was assigned to the Child Exploitation Investigations Group for the HSI Office of the Special Agent in Charge, Los Angeles, California ("HSI Los Angeles"). In November 2014, I was transferred to the Child Exploitation Investigations Group for the HSI Office of the Assistant Special Agent in Charge, Riverside and San Bernardino, California ("HSI Riverside"). My daily duties as an HSI special agent include investigating criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. During the course of these investigations, I have participated in the execution of numerous search warrants and seized evidence of such violations.

2. Through my training and experience, I have become familiar with the methods of operation used by people who sexually exploit children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. This training and my experience in

these investigations have given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application for a search warrant for a residence in connection with a child pornography investigation. The residence to be searched is 12959 Lasselle Street, Moreno Valley, California (the "SUBJECT PREMISES"), which is described below and in Attachment A, which is hereby incorporated by reference.

4. The items to be seized are specified in Attachment B, which is hereby incorporated by reference. These items constitute evidence of violations of Title 18, United States Code, Sections 2251(a) (production of child pornography), 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) (together, the "TARGET OFFENSES").

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. BACKGROUND REGARDING CHILD EXPLOITATION OFFENSES, COMPUTERS, AND THE INTERNET

6. In this affidavit, "child pornography," "visual depiction," "minor," and "sexually explicit conduct," are defined as set forth in Title 18, United States Code, Section 2256.

7. Computers. Based on my knowledge, training and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

8. The development of computers has changed this; computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can now transfer photographs from a camera onto a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

11. Internet. The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state.

12. Internet Service Providers. Any individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or

Instrumentality Protocol

other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format.

13. IP Addresses. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

14. When a customer logs into the Internet using the service of an ISP, the computer used by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period.

IV. SUMMARY OF PROBABLE CAUSE

15. As set forth in greater detail below, Special Agent Patrick McCall of HSI Wilmington, Delaware ("HSI Wilmington") conducted an investigation into a popular mobile communication application, Kik Messenger, that was being used by many individuals to view and trade child pornography. In October 2015, agents from HSI Wilmington found that the Kik Messenger user "CM8JIAW4" posted images depicting the sexual exploitation of children to a Kik Messenger chatroom titled #NEPILOVERS. SA McCall subsequently identified the internet service account used by CM8JIAW4 as belonging to an Angelo Harper at the SUBJECT PREMISES.

V. STATEMENT OF PROBABLE CAUSE

A. KIK MESSENGER APPLICATION

16. According to my knowledge, training and experience, the Kik Messenger application is primarily a social media mobile device platform designed and managed by Kik Interactive Inc., a company based in Waterloo, Canada, for the purpose of mobile messaging and communication. To use this application, a user downloads the mobile messaging application via an applications service such as the Google Play Store, Apple iTunes, or other similar mobile application provider. Once downloaded and installed, the user is prompted to create an account and a username. This username will be the primary account identifier. The user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik Messenger users are

asked to supply a valid email address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by other users. Once the Kik Messenger user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik Messenger users can send messages, images, and videos between the two parties.

17. According to my knowledge, training and experience, Kik Messenger also allows users to create chatrooms, of up to 50 people, for the purpose of communicating and exchanging images and videos. These rooms are administered by the creator who has the authority to ban and remove other users from the created room. According to Kik Interactive Inc., more than 40% of the Kik Messenger users chat in "groups" and approximately 300,000 new groups are created every day. These groups are frequently created with a "hashtag" allowing the group or chat to be identified more easily. Once the group or chat is created Kik Messenger users have the option of sharing the "link" with all of their contacts or anyone they wish.

18. According to my knowledge, training and experience, Kik Messenger users frequently advertise their Kik Messenger usernames on various social networking sites in order to meet and connect with other users. In some cases, Kik Messenger also provides various avenues, such as dating sites and social media applications, for meeting other users.

19. Special Agent Patrick McCall told me that based on his experience and investigations involving Kik Messenger, many of the users stated they felt safe using Kik Messenger as a means of trading child pornography and for other illegal activities due to the fact that "Kik is a Canadian based company and not subject to the same United States laws." During the course of his investigation, SA McCall told me that he has noted messages posted in Kik Messenger chatrooms relating to the enforcement, deletion, or banning of users and rooms by Kik Messenger for the purpose of exchanging or distributing child pornography. SA McCall told me that he has noted that Kik Messenger users commented that they created new rooms and new user accounts to circumvent Kik Messengers enforcement efforts.

B. IDENTIFICATION OF "CM8JIAW4"

20. SA McCall told me that on October 8, 2015, at approximately 10:38 A.M. (EDT), SA Patrick McCall used a device connected to the Internet and logged into an undercover Kik Messenger account. SA McCall subsequently accessed the Kik Messenger chatroom titled "#NEPILOVERS," which contained the caption "All the things toddler n nepi." In reviewing the postings made in the #NEPILOVERS chatroom, SA McCall found that between August 26, 2015 and October 8, 2015, the Kik Messenger user "CM8JIAW4" posted at least five images and one video. I reviewed these images and the video and concluded, based on my training and experience, that they depicted child pornography. (Three of these images are described below.) SA McCall was able to successfully download, to an undercover device, the video and

three images posted by CM8JIAW4 on or about October 7, 2015. CM8JIAW4 Kik Messenger's profile picture depicts a computer generated silhouette of a male which is also the default image Kik Messenger users have when a profile picture has not been uploaded or assigned by the Kik Messenger user.

21. SA McCall told me that on or about October 8, 2015, he sent a summons to Kik Interactive Inc. requesting subscriber account information for Kik Messenger user "CM8JIAW4."

22. SA McCall told me that on or about October 12, 2015, Kik Interactive Inc. responded to the summons providing numerous login records and subscriber information. I personally reviewed the login and subscriber information, part of which is detailed below:

User name: CM8JIAW4

First name: Bobby

Last name: Green

Email: fakestofemail@fakermails.com (unconfirmed)

Location: US

Registered: 2015/04/15 19:08:35

Device: Android

23. The login records provided by Kik Interactive Inc. showed that between September 13, 2015 and October 11, 2015, the Kik Messenger account CM8JIAW4 was accessed approximately 28 times. Each time the CM8JIAW4 account was accessed, the user did so from the IP address 104.175.141.234 ("TARGET IP"). SA McCall conducted a query of the TARGET IP within the Maxmind.com online database. Maxmind.com is a publicly accessible database

that is regularly used by law enforcement to identify the owners of IP Addresses. In my experience, Maxmind.com is a reliable database. SA McCall told me that he learned that the TARGET IP is registered to the internet service provider ("ISP") Time Warner Cable.

24. SA McCall told me that on October 13, 2015, he sent a summons to Time Warner Cable requesting subscriber information for the TARGET IP utilized on October 7, 2015 at approximately 10:07 P.M. EST (GMT-0400), the date and time the TARGET IP was used by CM8JIAW4 to post three images of child pornography to Kik Messenger chatroom #NEPILOVERS.

25. SA McCall told me that on or about October 13, 2015, Time Warner Cable responded to the summons. I reviewed the records provided by Time Warner Cable. Time Warner Cable reported that the TARGET IP is assigned to an Angelo Harper at the SUBJECT PREMISES.

26. SA McCall told me that on October 13, 2015, SA McCall conducted various searches on the Internet for Angelo Harper and, among other things, found that Angelo Harper (DOB: April 15, 1958) is a registered sex offender.

27. According to my training and experience, the Megan's Law database is a database maintained by the California Department of Justice containing the physical address of registered sex offenders. On October 13, 2015, I searched the Megan's Law database for the SUBJECT PREMISES, which yielded a single result for Angelo Harper (DOB: April 15, 1958). According to the Riverside County Judicial Access court imaging system,

which I reviewed on October 13, 2015, Angelo Harper (DOB: April 15, 1958) was convicted in 1991 of a violation of California Penal Code 288(c), lewd act with a child under 15; case number CR41838. Angelo Harper (DOB: April 15, 1958) is required to register as a sex offender as a result of this conviction.

28. On or about October 13, 2015, I reviewed information provided by SA McCall relating to the Kik Messenger user CM8JIAW4. This information included, among other things, summons responses from Kik Interactive Inc. and Time Warner Cable and screen captures of CM8JIAW4 postings to the Kik Messenger chatroom #NEPILOVERS. I also reviewed the images, video and chat postings that CM8JIAW4 made to the #NEPILOVERS chatroom. Below is a description of three images CM8JIAW4 posted on October 7, 2015 at approximately 10:07 P.M. EST (GMT-0400):

a. The first image depicts a prepubescent male infant, appearing to be under the age of two years old. The child appears to be lying on his back looking up towards the camera. The child is wearing a red and white striped shirt and appears to be wearing a white and blue "onesie" underneath. The child's t-shirt and onesie have been lifted up exposing the child's abdomen. The child's diaper has been removed exposing his penis and anus to the camera. A male adult's penis is visible in the photo and it appears to be anally penetrating the child. A semi-transparent penis-shaped object is lying on top of child's chest.

b. The second image depicts what appears to be a prepubescent male infant, appearing to be under the age of two years old. The infant appears to be crawling, away from the camera, on the floor towards a toy that is just beyond his reach. The child is wearing a dark blue or black onesie that has been unbuttoned and lifted up. Similarly, the child's diaper has been lowered exposing the child's buttocks. The left hand of a male adult is seen in the photo hold an erect penis directly over the child's buttocks. The male adult appears to be wearing a black long sleeved shirt.

c. The third image depicts what appear to be the same prepubescent male infant and male adult. The image depicts an infant child, appearing to have on the same onesie as the one described above, and the male is wearing the same long sleeved shirt described above. The child is facing away from the camera and the child's diaper has been pulled aside. The left hand of a male adult is seen spreading apart the child's buttocks exposing the child's anus to the camera.

29. The three images detailed, posted on Kik Messenger by CM8JIAW4 on October 7, 2015 at approximately 10:07 P.M. EST (GMT-0400), were all posted with the header "camera." Based on my training and experience with Kik Messenger, I know that Kik Messenger offers several ways to post an image. A Kik Messenger user can either upload a preexisting image from the device's gallery or photo album or use the device's camera to post directly to Kik in real time. When a Kik Messenger user posts directly to Kik in real time using the device's camera, the

image is given the header "camera." Therefore, since the three images above have the header "camera," I believe that the images described above were likely posted on Kik Messenger contemporaneously with the images posted by the same person who took them.

30. On October 13, 2015, I learned that on January 16, 2014, SA Dayna Roelfs of HSI Riverside executed a federal search warrant at the SUBJECT PREMISES, in Case No. ED 14-0025M. The search warrant was for evidence of violations related to the possession, distribution and receipt of child pornography. On October 13, 2015, I spoke with SA Roelfs about her investigation and learned that at the time SA Roelfs executed the search warrant, Angelo Harper (DOB: [redacted] and his son, Angelo Harper Jr. (DOB: [redacted] ("HARPER JR.") both resided at the SUBJECT PREMISES.

31. SA Roelfs told me that during her interview with HARPER JR., HARPER JR. admitted to using Kik messenger and receiving hyperlinks to child pornography files contained on Dropbox.com, the online storage provider. HARPER JR. also admitted to having an interest in children under the age of 10 years old. HARPER JR. stated that he thought he would not lose interest in child pornography.

C. THE SUBJECT PREMISES

32. On October 13, 2015, at approximately 1:45 P.M., SA Steve Marin arrived at the SUBJECT PREMISES. SA Marin found parked in the driveway of the SUBJECT PREMISES a HONDA with California license plate [redacted]. Records checks conducted

within databases maintained by the California Department of Motor Vehicle ("DMV") revealed that the vehicle is registered to Mariah Harper, Angelo Harper's daughter, at the SUBJECT PREMISES.

33. On October 13, 2015, I checked databases maintained by DMV and learned that HARPER JR.'s current address of record as indicated in his driver's license is the SUBJECT PREMISES.

D. TRAINING AND EXPERIENCE ON CHILD PORNOGRAPHY INVESTIGATIONS

34. Through my training and experience, I have become familiar with the methods of operation used by people who sexually exploit children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. This training and my experience in these investigations have given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses.

35. I have been the case agent on and assisted with more than 100 cases involving the sexual exploitation of children. I have worked cases involving Peer-to-Peer networks where individuals have used the internet and file sharing software to distribute child pornography. I have worked cases involving individuals who travel to foreign places to engage in sexual conduct with minors and/or produce child pornography. I have also worked cases where individuals have used the internet to

entice or induce minors to produce child pornography some of which involved applications like Kik Messenger. In my training and experience, I have found that individuals who use Peer-to-Peer or other internet platforms to trade child pornography frequently use more than one such internet platform.

36. In my experience, individuals who collect child pornography frequently also collect "child erotica," which although not technically child pornography depicts children in settings and manner which are sexually suggestive. In my training and experience, I believe that a person's possession of child erotica tends to demonstrate that they are sexually interested in minors.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

37. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information

related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to

search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or

recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has

been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the

absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

38. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

///

///

///

VII. CONCLUSION

39. For all the reasons described above, there is probable cause to believe that evidence of violations of the TARGET OFFENSES, as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

Jonathan Ruiz, Special Agent
Homeland Security
Investigations

Subscribed to and sworn before me
this 13th day of October, 2015.

THE HONORABLE DAVID BRISTOW
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises located at 12959 Lasselle Street, Moreno Valley, California (the "SUBJECT PREMISES"), further described as follows:

The SUBJECT PREMISES is a single story residence located on the west side of Lasselle Street, just north of Eucalyptus Avenue and south of Fir Avenue. The front door of the SUBJECT PREMISES faces east. The SUBJECT PREMISES is beige in color with a clay tiled roof and green trim. The residence has a two car garage with a roll up door and four small windows at the top. The residence has a white security screen door. The numbers "12959" are painted on the curb in black just to the left of the driveway entrance.

The areas to be searched include (a) all rooms, porches, containers, and safes in the SUBJECT PREMISES; (b) any other parts of SUBJECT PREMISES, including its driveway, and any garages, carports, storage spaces, or other outbuildings on the SUBJECT PREMISES; and (c) any and all vehicles parked on or in front of the SUBJECT PREMISES, provided that such vehicles are registered to or under the control of individuals residing at the SUBJECT PREMISES.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), namely:

a. Records, documents, programs, applications, or materials which contain child pornography, as defined in Title 18, United States Code, Section 2256(8).

b. Records, documents, programs, applications, or materials concerning the possession, receipt, distribution, advertisement, and/or reproduction of child pornography, as defined in Title 18, United States Code, Section 2256(8).

c. Records, documents, programs, applications, or materials concerning the viewing, sharing purchasing, or downloading of child pornography, as defined in Title 18, United States Code, section 2256(8).

d. Records, documents, programs, applications, or materials concerning any production, receipt, shipment, order, request, trade, purchase, or transaction of any kind involving the transmission through interstate commerce by any means, including by computer, or any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, section 2256(8).

e. Records, documents, programs, applications, or materials concerning identifying persons transmitting any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, section 2256(8).

f. Records, documents, programs, applications, or materials that identify any minor visually depicted while engaging in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8).

g. Records, documents, programs, applications, or materials which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, missing children, investigative techniques of child exploitation, sexual disorders, pedophilia, nudist publications, diaries, and fantasy writings.

h. Records, documents, programs, applications, or materials that pertain to P2P file-sharing software.

i. An infant/toddler-sized red and white striped shirt.

j. An infant/toddler-sized white and blue "onesie".

k. An infant/toddler-sized dark blue or black onesie.

l. An adult-sized black long sleeved shirt.

m. Any records, documents, programs, applications, or materials that pertain to accounts with any Internet Service Provider.

n. Any digital device used to facilitate the above-listed violations and forensic copies thereof.

o. With respect to any digital device used to facilitate the above-listed violations or containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical

disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

4. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of the warrant. If additional time is needed, the government may seek an extension of this time period from the Court on or before the date by which the search was to have been completed.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to

determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use sophisticated hashing tools, such as tools for identifying child pornography, including "EnCase" and "FTK" (Forensic Tool Kit).

c. When searching a digital device pursuant to the specific search protocols selected, the search team shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

f. If the search determines that a digital device does contain data falling within the list of items to be seized,

the government may make and retain copies of such data, and may access such data at any time.

g. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of items to be seized, the government may retain forensic copies of the digital device but may not access them (after the time for searching the device has expired) absent further court order.

h. The government may retain a digital device itself until further order of the Court or one year after the conclusion of the criminal investigation or case (whichever is latest), only if the device is determined to be an instrumentality of an offense under investigation or the government, within 14 days following the time period authorized by the Court for completing the search, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending). Otherwise, the government must return the device.

i. Notwithstanding the above, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

a. Any digital device capable of being used to commit, further or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;

c. Any magnetic, electronic, or optical storage device capable of storing digital data;

d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.